Identity Theft Prevention

Prepared for:
Hardy Merritt
Certified Public Manager Program

Prepared by:
Sarah Niegsch, CPA
South Carolina Retirement Systems
December 16, 2003

I. Problem Definition

There is increasing coverage in the news media concerning "identity theft", which is the act of assuming another person's identity to commit financial fraud or other types of criminal activity. Identity theft begins when the perpetrator of the crime gains access to the victim's personal demographic information. The incidence of identity theft is increasing in our nation and in our state.

The South Carolina Retirement Systems (SCRS) administers the four defined benefit pension trust funds of the State of South Carolina. Our systems provide lifetime retirement annuities, disability benefits and death benefits to eligible members derived from a legislatively defined formula based on years of service, compensation and age. The SCRS also administers a defined contribution retirement plan, which is an alternative to membership in the traditional SCRS defined benefit plan. Therefore as a result of our business functions, the SCRS captures personal demographic information for every member and beneficiary of our system. Our records are kept under social security number and correspondence to members and beneficiaries includes social security number, as well as other demographic information.

The mission of the SCRS is to administer a comprehensive program of retirement benefits responsive to the needs of public employees and to perform fiduciary duties as stewards of the contributions and disbursements of the pension trust funds. Our vision is to empower our employees to provide

comprehensive service in a professional manner for our members, employers, and retirees through timely and accurate processing of payments, claims, inquiries, and other account information using effective and appropriate leading edge technology. Protecting our members from identity theft can be seen as part of our vision for providing quality customer service and as part of our mission to perform fiduciary duties as stewards of the contributions and disbursements of the pension trust funds.

The purpose of this project is to explore potential methods of protecting demographic information and recommend a proposed solution and implementation plan. The protection program must be implemented consistently agency wide and, because we are part of the larger entity of state government, should incorporate elements of the state's identity protection plan, if one exists. The plan will affect how we communicate with members, how we dispose of waste and our internal, automated database systems.

II. Data Collection

Identity theft, which has claimed 27.3 million American victims over the last five years, is the act of assuming another person's identity to commit financial fraud or other types of criminal activity, leaving the unknowing victim to face the consequences of the perpetrator's actions (FTC; Law Enforce). In the last year, identity theft has affected 9.9 million people and caused $53 billion in expense for

financial institutions and consumers (FTC). In 2002, identity theft complaints accounted for 43% of complaints registered with the FTC (Business Week). The numbers of complaints registered with the FTC rose by 88% from 2001 to 2002 (Business Week) and approximately 38% of consumers have been victims of identity theft (Law Enforce). In South Carolina in the period from January 1 through December 31, 2002, 1,239 cases of identity theft were reported, which ranks South Carolina 35th in the nation for number of victims per capita (FTC2). The most common type of identity theft in the United States as a whole and in South Carolina in particular is credit card fraud, which comprises 42% of reported thefts (FTC2). Phone and utilities fraud account for 22% of reported thefts (FTC2).

Obviously, identity theft is a common, increasing problem for the citizens of our country and of our state. As a state agency, the SCRS has recognized the vulnerability of our membership in this regard and has made it a part of our strategic plan to implement an identity theft prevention program. This purpose of this paper is to explore phenomenon of identity theft, examine the causes of it, and recommend a specific implementation plan for identity theft prevention for the SCRS.

The first step in developing an identity theft prevention program is to recognize that the problem exists. The statistics presented above clearly indicate a problem. However, in order to develop a feasible solution, we must understand

how identities are stolen. In cases of identity theft, assailants obtain the victim's personal demographic information such as name, address, social security number (SSN) or date of birth. Thieves then use this information to set up credit cards, utilities, phones, mortgages or other types of financial products in the victim's name. They often immediately change the billing address on the accounts so that the victim never knows the accounts exist. The victim may learn about the crime by monitoring their own credit report and accounts, by notification from a financial institution or collection agencies, or when until they apply for a loan or credit card and are rejected (FTC).

According to the FTC, 51% of victims know how their personal information was obtained. Stolen credit cards, checkbooks and social security cards account for 25% of cases. Stolen mail is the source of 4% of identity theft (FTC). Thieves can also gain information by "hacking" into automated database systems and web-based applications which house personal demographic information.

Identity theft can strike anyone. There are, of course, many levels of prevention that should take place to protect each individual's identity. Individuals should shred any trash that contains personal or financial information before discarding it. Individuals should also protect any passwords and account numbers and check their credit reports annually to ensure their accuracy. Businesses should also protect consumers' personal and financial information. This should be done both by taking technical precautions to ensure automated systems are not

compromised and by limiting the amount of personal information that is displayed on receipts and other written communication originating from the business.

As the administrator of the pension trust funds of the State of South Carolina, the SCRS is a storehouse of personal and financial information for our members and our beneficiaries. Each member and beneficiary is identified on our automated systems by SSN. The State of South Carolina, through the Architecture Oversight Committee coordinated through the Office of the Chief Information Officer, is currently reviewing information technology protocol related to identity theft protection. Although the committee has not yet published guidelines concerning identity theft, I feel that their study will encompass recommendations especially focused on information technology. Due to this factor and because I am an administrator and not an information technology expert, the focus of this project is to develop detailed guidelines for implementing a change in our external mailings to include less personal demographic and financial information and to start a program of education for our members – not recommendations related to our automated database administration.

The business functions of the SCRS are to track incoming financial information for each of our members and to eventually pay a benefit to the members or their beneficiaries based upon those contributions and the amount of time worked. Until 1975, as an agency we tracked member information based on an ARN number, which was a number generated at our agency. Over the years, we

collectively found it difficult to contact members once they had left our system, as members often didn't remember their number. Also, the ARN was a meaningless piece of information outside our system so it was of no use in locating members once they were no longer actively participating in our system. In 1975, the decision was made to change the administratively difficult process of tracking information by an agency-generated number to tracking information by SSN. It is nearly unanimous in the agency that changing from this tracking system to an SSN tracking system was beneficial administratively. So, although we want to protect our membership against the threat of identity theft, due to the ease of administration when compared with our prior tracking mechanism, we want to maintain our current database administration policy of tracking information by SSN.

Our current database systems are as follows. First, we have an automated Unix based custom written and in-house maintained database that contains personal demographic and financial information for members and beneficiaries. This system is used to record incoming contributions and service credit; to process retirement, refund and death claim applications; and to create and track payments. We also use an automated imaging system (scanning system) to store and access all information submitted to our agency via paper. For example, when a member completes a paper enrollment form, we enter the data into our Unix system and then have the document imaged. The scanned image of the document is then stored under the SSN and may be accessed along with

any other paperwork that has been imaged under that same SSN by any employee in the agency who has the appropriate access to do so. Both the Unix and the Imaging systems currently work very well and facilitate an efficient workflow. Unix and Imaging are correlated in that correspondence generated in Unix can be automatically stored in imaging.

Currently, all external mailings to members include the member's SSN as well as name and address. Many of these external mailings are pre-printed with information and expected to be returned to our office for further processing. We also commonly print and discard many documents as a result of on-going business functions. Because we do deal with personal demographic information, much of our waste contains information that could be used to perpetrate identity theft. We currently do not shred any discarded documents in house. All of our paper recycling is disposed of by the Department of Corrections of the State of South Carolina. Our trash service is a non-secure disposal service.

III. Proposed Solutions

As noted previously, 4% of identity theft victims know their personal information was accessed through stolen mail. Currently, the SCRS includes SSN as well as name and address on all of our outgoing mail to members. The SCRS can lessen the risk of identity theft for its members by modifying outgoing mail communications to not include SSN.

Administratively, because the majority of our external mailings are eventually returned to us for future processing and because all of our automated programs are accessed and information is stored by SSN, it is much easier for us to process documents when they are returned to our office if the SSN is present on the document. Two options have been explored to minimize exposure of our membership in our external mailing and yet include enough identifying information for us to process the document upon return to our office. The first would modify outgoing communications to include only the last four digits of the SSN; the second, to include a bar code encrypted with the member's SSN.

In order to implement the first scenario of including only the last four digits of the SSN on the external mailing, our automated programs would need to be modified to create a browse on-line to derive the entire SSN from the first four digits of the last name and the last four digits of the SSN. An analysis of our entire database, including active members, retirees and beneficiaries, identified that approximately 7% of our population will not have a direct match based on those two criteria. In those instances, our staff will have to determine the proper SSN from other available data such as address or date of birth, which will require additional time upon processing a returned document. Another aspect of this approach is that our imaging department stores all images under SSN. The process in our imaging department is like an assembly line; any time someone in the imaging department has to stop the actual process of imaging to identify an

SSN, the total work inflow of the department halts until the SSN is identified. Because documents will no longer have the entire SSN printed on them, if this scenario is chosen, we will need to ensure that documents that have been modified to include only the last four digits of the SSN go directly to imaging rather than being printed and hand carried to imaging.

The scenario of placing a bar code encrypted with the SSN of the member on external mailings would also require modifications to our automated systems. If a bar code were printed on each external mailing, when a document is returned to our office for further processing, our employees could simply scan the bar code to determine the entire SSN, which would eliminate any further research to uniquely identify the member. Also, if a document were forwarded to imaging, as long as the department possessed the required bar code reader, employees would simply be able to scan the document to determine the entire SSN and image accordingly. However, bar-code readers would have to be purchased for each employee processing turn-around documents, employees in imaging and high-quality printers would have to be used to print external mailings to ensure the readability of the bar-codes. Also, employees would the ability to create bar codes for manual, one-time letters. Our information technology staff advised that the automated changes required to complete the bar code project would be more time consuming than the changes required to implement the first scenario.

As another proposed solution, because not all of our internal printed documents are external mailings, even if one of these scenarios is initiated, we still have documents containing personal demographic information to be discarded. Our recycling disposal process is administered by the Department of Corrections. It is a secure process that is bonded and documents are shredded by them after pick up. Our trash disposal service; however, does not provide similar security. Therefore, I recommend that we ensure all staff recycle any documents that contain personal demographic information. This step could be provided at no cost to our agency.

Another identity theft prevention tool that could be provided at no cost is to include an article on identity theft protection in our next newsletter, which is distributed to annuitants and active members and to include the article on our website. The article should include the basic prevention tips for individuals such as shredding any trash that contains personal or financial information before discarding; protecting any passwords and account numbers; and checking credit reports annually to ensure their accuracy.

I also recommend that as an agency we periodically check the progress of Architecture Oversight Committee to ensure we are in compliance with eventual State guidelines and to take advantage of additional insights concerning the issue of identity protection in relation to administrative and technical procedures.

The benefit to implementing a program of identity theft protection is an intangible one. We will be providing additional customer service for our membership in that their personal demographic information will be more secure than under our previous procedures. The benefit of this is impossible to measure because we will never know exactly what types of crimes we will have prevented and what dollar amounts are associated with the prevention. There is also the intangible benefit of public relations if a case of identity theft were ever to be linked directly to information disseminated from our office. We have already received numerous requests from members inquiring about our identity theft protection procedures. To be able to specifically outline steps we are taking to ensure the security of our data will be a public relations benefit to our agency.

IV. Results

In December of 2003, our agency decided to implement an identity theft prevention program that will entail changing external mailings to include only the last four digits of the SSN. As we wanted to implement a prevention plan to protect our members as soon as possible, this was seen as a quicker and less costly alternative when compared to the bar-code idea (we will not have to purchase bar code readers and the programming changes to implement the bar code system required less time by our information technology staff). The automated changes will be implemented over a six-month period of time. A project is also currently underway to include an article in our next newsletter communicating what we are doing as an agency to protect against identity theft

and what individuals can do to protect themselves. Management has been advised of my recommendations to ensure all discarded documents containing demographic information are recycled and not discarded in the trash and that as an agency we should monitor the progress of the Architecture Oversight Committee.

Bibliography

Federal Trade Commission. "FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers. Media Release. September 3, 2003. www.ftc.gov/opa/2003/idtheft.htm.

Federal Trade Commission. "Identity Theft Victim Complaint Data. Figures and Trends in South Carolina, January 1 – December 31, 2002. January 22, 2003. www.consumer.gov/sentinel/

Federal Trade Commission. Official Identity Theft Website. www.consumer.gov/idtheft.

"Identity-Theft Study Says Crime Is on the Rise". Wireless News. May 15, 2003.

Pollock, John and May, James. "Authentication Technology: Identity Theft and Account Takeover". Law Enforcement Bulletin. June 2002, Volume 71, Number 6.

Salkever, Alex. "To Thwart the Identity Thieves". Business Week Online. February 11, 2003.

South Carolina Budget and Control Board, Division of the State Chief Information Officer. "Architecture Oversight Committee". www.cio.sc.gov.